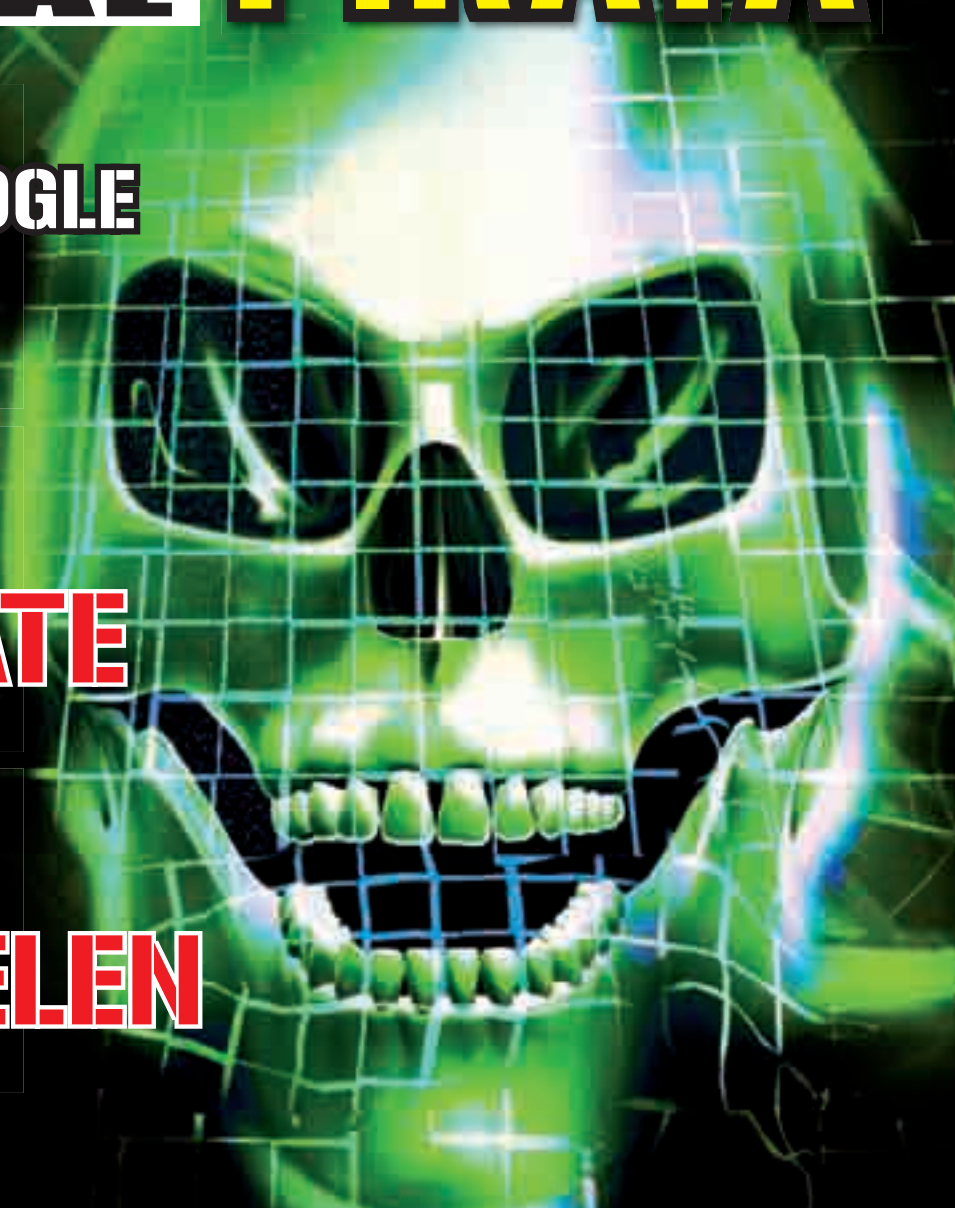
TUTTO QUELLO CHE GLI ALTRI NON DICONO
NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
2€
n.190
HACKER
JOURNAL
www.hackerjournal.it
CRACKING
WINDOWS 7
PIRATA
PROGRAMMING
REGALI DA GOOGLE
CLOSURE
ATTACCHI
TRANSAZIONI
SSL BUCATE
ESCLUSIVA
INTERVISTA A
MICHAEL BOELEN
QUATTORD. ANNO 9 - N° 190 - 4 DICEMBRE / 17 DICEMBRE 2009 - € 2,00
FOCUS ON
CLOUD COMPUTING VS SECURITY
PGP NON È PIÙ SICURO

Anno 9 – N.190
4 dicembre / 17 dicembre 2009

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

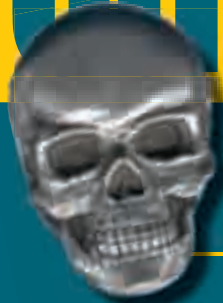
Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

Hacker dovunque

"La gente dice che dovrei accettare il mondo. Stronzate! Io non accetto il mondo." (Richard Stallman, discorso al New York Linux Bazaar)

Il dibattito su cosa considerare "roba da hacker" sta andando avanti, ormai, fin dagli anni '50 quando, al MIT di Boston, il termine hack era sinonimo di goliardico. Un problema impegnativo, questo, per chi scrive su una rivista come la nostra, i cui confini di interesse dovrebbero essere ben definiti. Purtroppo, però, per sua stessa natura, l'hacking non può avere confini netti. Sicuramente non siamo tutti d'accordo nel dire che l'hacker ha a che fare solo con l'informatica e quelli che hanno questa convinzione sono ormai una minoranza.

Una installazione artistica in cui una webcam viene usata per rielaborare le tracce lasciate dalla polvere e ottenere quadri casuali è un'operazione di hacking? Un manipolatore che sfrutta le debolezze altrui per compiere una truffa è un hacker? Un ragazzino che smonta il televisore per capire come funziona, è un hacker? Domande a cui dare una risposta è complicato dal fatto che ogni giudizio risulta frutto di considerazioni ecniche ma anche delle idee personali di chi giudica.

Noi, a modo nostro, questa risposta l'abbiamo ed è quella di intendere le cose in modo ampio. Non è più il tempo dell'hacker equiparato al topo da sala server, un po' sfigato, che vede raramente la luce del sole e si occupa solo di computer.

Quello è lo stereotipo dell'hacker e non può andarci bene. L'hacker, oggi, è una persona come tante altre, che cerca di ottenere un livello superiore di comprensione delle cose ed è per questo che ogni nostro numero spazia dalla programmazione alla cultura, da considerazioni sociali a quelle legali.

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ: mandateci una mail!
Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa.
Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

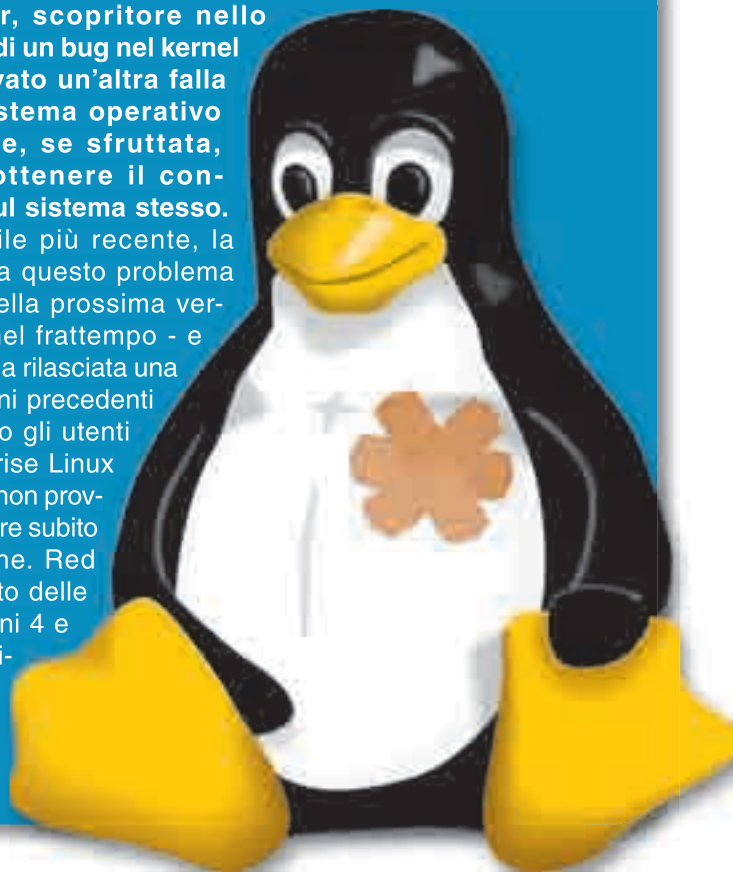
Benedetti ragazzi!

Si è conclusa il 15 novembre una tre giorni che ha visto coinvolta l'assemblea plenaria della Commissione Episcopale Europea per i Media. Non stiamo parlando di qualche raduno underground in un paesino sperduto ma di una riunione che ha visto come protagonisti alti prelati della Chiesa Cattolica che, con il supporto dei rappresentanti dei siti più consultati (Facebook, YouTube e Wikipedia) e la partecipazione di esperti di sicurezza (tra cui esponenti dell'Interpol) ha visto confrontarsi un mondo considerato antiquato come quello ecclesiastico con le nuove tecnologie. Attenzione: quello che considera antiquata la Chiesa è, da tempo, niente più che uno stereotipo. L'attenzione verso le nuove forme di comunicazione, la sperimentazione e la testimonianza di fede tramite media innovativi non sono cose recenti. Basta pensare che Radio Vaticana venne inaugurata nel 1931 niente meno che da Marconi in persona. Da allora è passato molto tempo e il mondo della comunicazione è cambiato, facendo cambiare anche uno degli apparati religiosi più grandi al mondo. Oggi, i preti navigano sul Web, scambiano mail col vescovo, fanno telefonate VoiP con i "loro" missionari, offrono Internet wireless in qualche oratorio e molti proseguono la loro opera persino sui social network, Facebook in testa. Una voglia di innovazione e adeguamento ai nuovi sistemi di comunicazione che arriva dal passato e che viene stimolata dal Papa in persona.
Da qui l'esigenza di un confronto di questo mondo con esperti delle nuove tecnologie su temi ovviamente inerenti all'opera pastorale: dalla presenza della Chiesa sul Web al modo in cui i giovani usano Internet, dall'uso della Rete per lo sviluppo della fede fino alle questioni legate al copyright e alla privacy.
Inutile dire che, trascurando gli aspetti religiosi, un interessamento così dettagliato e di vasta portata non potrà che giovare alle discussioni in atto, in tutto il mondo, sui temi che più ci stanno a cuore: dalla difesa della privacy alla lotta per la tutela degli individui davanti allo strapotere, economico, delle Major. Nel frattempo possiamo registrare con soddisfazione un dato di fatto che rende questo mondo migliore per tutti: tra i sostenitori del software libero, la Chiesa Cattolica e singole le istituzioni che la compongono (dai piccoli oratori alle missioni estere), fanno la parte del leone. Un po' perché si parla di software il cui costo non incide sulle loro già esangui casse ma anche perché la creazione e l'uso di software libero permettono la collaborazione e la cooperazione tra tutti i soggetti coinvolti: aziende, professionisti, utenti e programmatori.

VIRUS PEDOFILO

Non è la prima volta che ci capita di vedere casi analoghi ma la storia di Michael Fiola è davvero raccapricciante per chi spende tanto tempo davanti al computer. Nel 2008, il povero signore si è visto infettare il portatile e, senza rendersene conto, ha iniziato a lasciare in giro il suo IP su circa 40 siti pedopornografici al minuto. Un'attività del genere non poteva passare inosservata alle autorità che si sono quindi scagliate sul pedofilo con aggressività. 250.000 dollari di spese legali, un mutuo per pagare gli avvocati, la macchina in vendita, la perdita del lavoro, l'odio dei vicini e le minacce di morte. Tutto questo per poi vedersi scagionare completamente in fase di processo. Insomma, come se non l'avessimo mai ribadito, occhio a cosa fa e a cosa fate con il vostro PC. Basta un attimo per trovarsi in grane enormi.

IL CUORE MALATO DEL PINGUINO

Brad Spengler, scopritore nello scorso luglio di un bug nel kernel di Linux, ha scovato un'altra falla nel cuore del sistema operativo open source che, se sfruttata, può portare a ottenere il controllo completo sul sistema stesso. La versione stabile più recente, la 2.6.31, è affetta da questo problema che sarà risolto nella prossima versione, la 2.6.32; nel frattempo - e nell'attesa che venga rilasciata una patch per le versioni precedenti - i più esposti sono gli utenti di Red Hat Enterprise Linux (Rhel), a meno che non provvedano ad aggiornare subito le proprie macchine. Red Hat ha già rilasciato delle patch per le versioni 4 e 5 della propria distribuzione e presto un aggiornamento per la versione 3 sarà disponibile.

PHISHING 2.0

Symantec segnala un nuovo attacco di phishing che sfrutta la popolarità di Facebook per mettere in trappola gli utenti. I messaggi di phishing arrivano via email con l'esca di un improbabile aggiornamento ("Facebook account update", "New login system" e "Facebook update tool") e sono identici agli inviti ufficiali. Se un utente clicca su Update può essere reindirizzato su un sito fasullo che assomiglia a Facebook, dove si richiede di inserire la propria password; quest'azione autorizza il sito a rubare il codice di accesso. I consigli sono sempre gli stessi: prestare la massima attenzione agli allegati sospetti, soprattutto a quelli che includono una richiesta di "cambio password": nessun sito legittimo manderà mai una simile richiesta. Non cliccare su indirizzi sconosciuti senza averli prima verificati e, in ogni caso, è sempre bene copiarli sulla barra degli indirizzi. Installare sul computer un software antivirus aggiornato che protegga anche dai "malware da download".

UN VERME NEL MELAFONINO

Secondo Sophos si tratta del "primo worm per iPhone al mondo"; per il momento pare che la sua diffusione sia limitata all'Australia anche se, in teoria, nulla ne vieta l'esportazione in altre parti del pianeta. Possono essere infettati soltanto gli iPhone che sono stati "sbloccati", abilitando funzioni rese normalmente inaccessibili da Apple ma aprendo anche la porta ai pericoli. Il worm può infatti introdursi soltanto negli iPhone che i loro padroni hanno sbloccato senza cambiare la password di default dell'utente root (alpine), dopo l'installazione di Ssh, contravvenendo alle istruzione che spiegano come effettuare il jailbreaking. Se trova la porta aperta, il malware cambia lo sfondo mostrando una fotografia del cantante Rick Astley sormontata dalla scritta "ikee is never going to give you up", un riferimento alla canzone di Astley: Never gonna give you up. Poi si mette in cerca di altri iPhone da compromettere, diffondendosi.

BITTORRENT MENO ESOSO

I cosiddetti ISP (Internet Service provider), le compagnie che offrono accesso a Internet, si sono trovate da tempo a dover affrontare il problema legato a BitTorrent e alle grandi risorse in termini di banda che questi client richiedono. Il rimedio spesso più utilizzato è quello definito throttling: per riuscire a eliminare, almeno in parte, il problema, infatti, alcuni ISP hanno deciso di limitare il traffico dati su protocollo BitTorrent. Proprio per venire incontro a questo tipo di problematiche, BitTorrent inc ha sviluppato, nel corso degli ultimi anni una nuova versione del proprio protocollo di scambio dati, in grado di riuscire a risultare meno pesante e più adatto all'infrastruttura. Il nuovo protocollo non dovrebbe andare ad influire in modo diretto sulle velocità di download, invariate, quanto lavorare maggiormente sull'upload. I benefici saranno tangibili sia per l'utente, che non si vedrà costretto a battagliare con le impostazioni per riuscire a mantenere una navigazione fluida, sia per gli ISP.

KOOBFACE CAMBIA VOLTO

Trend Micro ha identificato una nuova evoluzione della botnet Koobface che, questa volta, colpisce il servizio Google Reader. L'attacco funziona attraverso un account Google controllato dal gruppo Koobface che propone una pagina con un finto video YouTube. Quando un utente clicca sul video fasullo viene rediretto a un sito Web compromesso che, a sua volta, contiene un altro finto video YouTube. Il sito compromesso infetta l'utente che diviene così parte inconsapevole della rete di Pc zombie Koobface. Al momento si ha prova di circa 1.300 account Google Reader fasulli usati da Koobface per questo scopo: i cybercriminali sfruttano, attraverso lo spam di collegamenti pericolosi, la funzione di condivisione dei nuovi contenuti.

Twitter: colpito e affondato

La resa è arrivata da Biz Stone in persona, il fondatore di Twitter: siamo sotto attacco. Infatti il servizio è andato in tilt, collassato per ore, afflosciandosi su sé stesso. In un post lanciato dallo stesso Biz, la resa è raccontata tra ironia e amarezza: "In questa mattina di giovedì, che sembrava tranquilla e felice, Twitter è finito sotto attacco. Attacchi di questo tipo sono vere e proprie iniziative dolose, orchestrate per rendere inutilizzabili servizi come le banche online, i sistemi di pagamento via web e, appunto, i sistemi di comunicazioni come Twitter. Ma noi ci difenderemo". Twitter si difenderà ma, per ora, l'attacco arriva proprio nel giorno in cui il social network è stato scelto dal presidente degli Stati Uniti, Barack Obama, per lanciare l'offensiva finale della grande battaglia per la riforma della sanità. Quello portato avanti dagli hacker è stato un attacco in piena regola, che ha costretto i gestori del network a sospendere il servizio. Dagli Stati Uniti all'Europa, il servizio elettronico è andato in tilt lasciando a piedi milioni di utenti: il server rifiutava gli accessi costringendo gli utenti a riavviare i computer per il pericolo di infezioni.

Banda larga

Stretta la banda... larga la via...

LA NOTIZIA

Il ministro Claudio Scajola, in una intervista a SkyTG24, ha rivelato che il Governo ha intenzione di finanziare lo sviluppo della banda larga entro la fine di quest'anno perché lo ritiene un investimento alla pari di quelli previsti per le infrastrutture materiali. Sono previsti investimento per 800 milioni di euro per aggiornare l'infrastruttura italiana.

Dite la vostra, io sto per dire la mia.... Scusate l'incipit da fiaba ma ormai qua ci manca solo di vedere i tre porcellini che tirano i cavi poi le abbiamo davvero viste tutte.
Sono anni che ci menano per il naso che arriveranno grandi investimenti per la banda larga, che saremo tutti cablati, che si stanziano fondi per le infrastrutture salvo poi, come sempre, rimangiarsi tutto all'ultimo momento. Andiamo avanti così da un bel po': ricordo di averne scritto proprio su queste pagine, forse un paio di anni fa, e le cose non sono cambiate per nulla. Cambiano i governi, i ministri, i parlamentari europei ma noi continuiamo ad avere infrastrutture informatiche degne del terzo mondo (con tutto il rispetto per i paesi che ne fanno parte e che, in alcuni casi, ci superano proprio su questo tema).
Insomma, l'ultimo tira e molla è stato sui famosi 800 milioni di euro che sarebbero stati stanziati per lo sviluppo della banda larga. Stanziati, poi se ne sono perse le traccie, poi il ministro Scajola dice che ci sono e si possono (si devono) usare, allora interviene Tremonti che dice che si ci sono ma sono destinati ad altro quindi se vogliamo la banda larga dobbiamo tagliare qualcosa d'altro, alla fine arriva Corrado Calabrò che propone di rivolgersi ai privati se lo stato non può farsi carico di questa spesa... Che colpo di genio!!!
Nessuno si domanda se i privati vorranno metterci tutti quei soldi e come faranno a guadagnarci?
Insomma, loro strillano, strepitano e noi rispolveriamo i modem a 56k, visto che, se va avanti così, con le centrali stracolme e al limite del collasso, giusto con quello potremo permetterci di navigare...
Buona notte e sogni d'oro a tutti.

BigG

di stato?

Non intendo sostenere che la banda larga non sia importante, anzi: secondo me è decisamente più importante di diverse altre infrastrutture. Se fosse veramente disponibile dovunque, un mio caro amico pugliese riuscirebbe finalmente a collegare alla Rete la sua webcam puntata sulla spiaggia dei nudisti e diversi di noi saprebbero come spendere meglio le loro giornate estive.

Purtroppo, però, la banda larga è un costo. Ai privati non frega nulla perché i privati vanno dove c'è reddito, dove è logico spendere decina di migliaia di euro per raggiungere un nucleo abitativo in cui recuperare abbonamenti che permettano di ammortizzare la spesa nel minor tempo possibile. Lo sa bene chi ha una casa isolata, magari in montagna, che non è stata raggiunta dal telefono quando la telefonia era affare di stato. Telecom, per molti versi ancora monopolista, non è più disposta a offrire il suo servizio al costo della sola attivazione ma in molti casi richiede contributi extra che possono raggiungere facilmente importi stratosferici: scavi, posa di tubi, fili... Un sacco di cosi che le aziende private non vogliono e non possono sobbarcarsi.

Pensiamo che in un'economia di mercato liberista come quella americana, la diffusione della Rete ha sempre goduto di finanziamenti statali sotto forma non solo di benefit fiscali alle aziende disposte a investirci ma anche in modo diretto, tramite costruzioni di reti in fibra da parte di istituzioni civili e militari. Alla fine, lo stato dovrà intervenire e tentare di risolvere il problema. In ogni caso, il mio vecchio 56K è al sicuro da qualche parte in cantina e le foto della spiaggia continuerò a farmele mandare tramite snailmail.

Khamul

La coperta è corta...

DÍ LA TUA

Sei d'accordo con la botta o con la risposta? Pensi che lo Stato debba investire oppure è un affare privato? Trovi che l'Italia dovrebbe essere completamente cablata oppure meglio rivolgersi ad altre tecnologie? Fai sentire la tua voce! Partecipa al dibattito sul nostro forum (www.hackerjournal.it) oppure scrivici all'indirizzo redazione@hackerjournal.it!

Google Gift

La grande G regala i suoi tool di sviluppo!

La notizia è di quelle che possono cambiare il modo di lavorare di molti sviluppatori: Google mette a disposizione i suoi strumenti di sviluppo, gratuitamente, a chiunque voglia creare applicazioni Web per la sua piattaforma.
Il cuore del sistema è il potentissimo Closure Compiler: un vero e proprio compilatore e ottimizzatore di codice Javascript. Il suo funzionamento è semplice quanto sono fantastici i risultati che offre. Un parser prende in carico il codice JS e lo analizza, eliminando parti di codice inutile e ottimizzando il resto. Il tutto facendo anche controlli di sintassi, di variabili e di tipo. Esattamente come avviene per i compilatori di normali linguaggi di programmazione, Closure Compiler fornisce un codice estremamente snello, compatto, ottimizzato e adatto a far girare sui client qualsiasi tipo di applicazione. Avere un'idea di quello che può fare è semplice: è lo strumento usato dagli sviluppatori interni della grande G e tutte le applicazioni che abbiamo a disposizione sulla sua piattaforma sono state realizzate con questo strumento. Le possibilità di utilizzarlo, inoltre, non sono limitate all'utilizzo come compilatore

CONVIENE?

La questione non è banale: dopo aver sviluppato un software piuttosto avanzato ad uso interno, con un certo dispendio economico, Google lo regala agli sviluppatori (ma non solo).
Non ci sarà qualcosa sotto? Ovviamente Google ha fatto bene i suoi calcoli: una piattaforma di sviluppo può crescere tramite risorse interne soltanto fino ad un certo punto. Oltre questo limite si rischia di investire in un ecosistema di software che fa perdere tempo e denaro. In più, senza il coinvolgimento diretto delle community di sviluppatori, qualsiasi grande software house rischia di non riuscire a far affezionare a sufficienza il mercato. Lo sa bene Microsoft che ha conquistato in passato tutto il conquistabile e sta cercando di mantenere il suo dominio con l'iniziativa TechNet: seminari gratuiti, corsi, software in regalo agli sviluppatori, accordi di partnership con software house più piccole e così via. Da questo punto di vista, la mossa di Google non fa altro che portare il piano del confronto con il colosso di Redmond sulla parità, dotando anche Google di una community di sviluppatori esperti nelle sue tecnologie. Staremo a vedere i risultati di questo scontro.

da riga di comando (funzionante in Java) ma si estendono alla possibilità di trattarlo come Web Application e come API. Come se non bastasse, è perfettamente integrabile da altri add-on che, su Firefox, permettono di avere un ambiente di sviluppo pressoché completo: controllo di debug (Firebug+Closure Inspector), controllo di velocità di upload delle pagine (PageSpeed), API (Closure Library) e template già pronti per iniziare (Closure Template).

:: Meraviglia!

I risultati dell'applicazione di Closure Compiler in semplici applicazioni JS sono buone ma non esaltanti. Nel caso di applicazioni complesse, tuttavia, i risultati migliorano sensibilmente, offrendo prestazioni difficilmente raggiungibili in altri modi. Il codice risulta molto più compatto, con file JS decisamente più piccoli: un vantaggio in più per chi sviluppa applicazioni sul Web e necessita tempi ragionevoli di download delle pagine. Il codice JS è, manco a dirlo, controllato nel dettaglio, riducendo sensibilmente i bug e i casi in cui vengono generati warning dal browser: ogni operazione rischiosa viene individuata dal parser e va approvata in modo specifico.
Ovviamente, Google ha previsto l'opportunità di testare sul campo il nuovo strumento da parte di chi non dispone di una infrastruttura adatta. Ogni compilazione eseguita prevede la registrazione di un file .js in hosting sui server della casa di Mountain View, richiamabile tramite un link fornito dal compilatore stesso. Questo resterà a nostra disposizione per circa un'ora, così da poter testare una situazione di produzione senza costi da parte nostra. Ovviamente, il file è accessibile in ogni momento e si modificherà nel caso di ritocchi al codice e nuove ottimizzazioni. Così facendo potremo avere una pagina Web, anche locale, che richiama il file remoto e controllare in continuazione, con un semplice refresh, il corretto funzionamento del codice. Sicuramente non abbiamo a che fare con un IDE ma poco ci manca.

Complessivamente, questa scelta di Google è un bel bocconcino per tutti quelli che, più o meno, hanno a che fare con la programmazione JS e confonde un po' i piani del suo principale concorrente nel campo (vedi box). Per noi appassionati è sicuramente un bel gioco ma anche l'occasione per realizzare applicativi web based di livello simile a quelli già esistenti nell'ambito off-line. Un passo (necessario) in più per il progetto di cloud computing verso cui la grande G vorrebbe far migrare tutti.

RIFERIMENTI

- **Closure Compiler**
code.google.com/intl/it-IT/closure/compiler/
Il cuore della piattaforma di sviluppo offerta da Google.
- **Firebug**
getfirebug.com/
Un debugger integrato per Firefox.
- **Closure Inspector**
code.google.com/intl/it-IT/closure/compiler/docs/inspector.html
Un add-on per Firebug che si integra in Closure Compiler e permette il debug delle applicazioni Google.
- **Closure Library**
code.google.com/p/closure-library/source/checkout
Una libreria Javascript che fornisce sia strumenti di base per la manipolazione di oggetti che widget avanzati in perfetto stile Google.
- **Closure Template**
code.google.com/intl/it-IT/closure/templates/
Una serie di template di base ed avanzati per velocizzare la creazione delle applicazioni della Google Platform, completamente personalizzabili.
- **Page Speed**
code.google.com/intl/it-IT/speed/page-speed/
Un plugin per Firefox che permette il controllo dei tempi di caricamento di una pagina Web, integrabile in Closure Compiler per un confronto di prestazioni.

Google Labs è la divisione di Google che studia nuove tecnologie, in cui qualsiasi programmatore trova risorse utili, sempre gratuite, per lo sviluppo di applicazioni.

Sono tantissimi i sistemi live su CD che risolvono i problemi più disparati

i CD di emergenza

Negli ultimi anni, forte anche dello sviluppo sempre maggiore del mondo Open Source, si è visto aumentare in modo deciso il numero dei Live CD dedicati ai compiti più diversi. Nella maggior parte dei casi, questi sistemi "live" sono dedicati al recupero dei dati da hard disk e supporti di memoria in genere, alla clonazione delle partizioni, alla diagnostica dei problemi hardware, all'analisi forense o addirittura al cracking "ragionato" delle password dei sistemi Windows.
Per quanto riguarda diagnostica hardware, recupero dei dati e clonazione di partizioni, vogliamo parlare di Parted Magic, un ottimo sistema live che può avviarsi sia da CD che da pendrive USB. Il sito del progetto è partedmagic.com. In questa distribuzione, fra i programmi più utili, troviamo Partimage, un utilissimo tool per lavorare sulle partizioni in modo estremamente flessibile: sono supportati i formati Windows (NTFS, FAT16 e 32), Linux (EXT2,3 e 4, Reiser, swap), Mac (HFS, HFS+) ma anche altri, meno conosciuti. Partimage consente di modificare le tabelle delle partizioni senza cancellare i dati, di verificare la presenza di partizioni nascoste e così via. Ricordiamoci che è sempre meglio

Usare il firewall di Linux, la distribuzione è Ubuntu in questo caso, è davvero semplice.

La lista delle distribuzioni Live è lunga e articolata e copre tutte le esigenze.

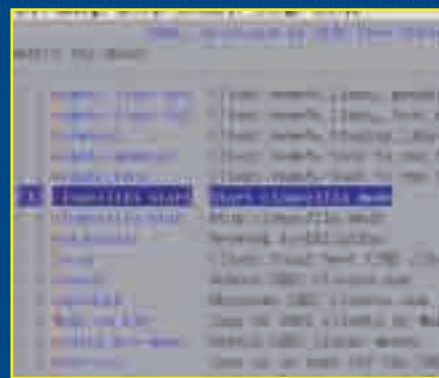
eseguire un backup dei dati prima di iniziare un'operazione di questo tipo. C'è anche Clonezilla, ottimo programma per la clonazione e il ripristino di dischi interi e partizioni singole. Clonezilla può lavorare sia su dischi locali che remoti, opera sulle singole partizioni e sui dischi fisici interi, supporta la maggior parte dei filesystem e, in ogni caso, può sfruttare la potenza del comando dd, che copia i dati in modalità byte per byte senza curarsi del filesystem. Clonezilla risulta estremamente utile in quei casi dove occorra clonare un sistema operativo per trasferirlo su un altro disco o partizione, senza quindi reinstallare tutto dall'inizio e preservando i dati. In PartedMagic abbiamo poi altre utility davvero comode, come Truecrypt, che permette di criptare con algoritmi a prova di bomba (AES-256, Twofish, Serpent) file, partizioni o interi dischi; inoltre Truecrypt risulta utile anche per rendere irrecuperabili i dati su un hard disk (pensiamo alla vendita del proprio PC oppure a scenari più ampi, per esempio il parco macchine di un'azienda che deve essere rinnovato e quindi viene solitamente venduto a basso prezzo per recuperare parte dell'investimento). La lista dei programmi è molto lunga e potete trovarla all'indirizzo partedmagic.com/programs.html.

:: Roba speciale

Alcune distribuzioni live sono orientate a compiti più specifici e meno "leciti" come, per esempio, OPHCrack, ophcrack.sourceforge.net. In poche parole, questo live CD (che può essere usato anche come un semplice programma stand-alone) si occupa di trovare le password di accesso dei sistemi Windows. Attualmente, il sistema più semplice da violare è Windows XP, seguito da Vista e, infine, dal nuovo arrivato Windows 7. Il vero problema di OPHcrack è che si basa sulle rainbow tables e queste sono molto ingombranti. Per Windows XP possiamo scaricare le tabelle XP Free small e fast, da 380 e 703 MB: dimensioni ancora accettabili. Per Windows XP versione tedesca, le tabelle occupano 7,4 GB, mentre per Vista si parte da 461 MB e si finisce con 134,6 GB! Le rainbow tables consentono un enorme risparmio di tempo in quanto contengono un elevatissimo numero di hash già pronti calcolati sulle parole più comuni usate come password. Di contro, lo spazio che occupano è davvero elevato. La percentuale di successo sfiora il 100%, a meno che la password da recuperare non sia superiore ai 12 caratteri alfanumerici.

:: Disastri!

Ultimate Boot CD è la soluzione definitiva alle esigenze di testing e benchmarking dell'hardware, ai problemi relativi ai dischi rigidi e a molto altro. Il CD è letteralmente pieno di utility di tutti i tipi. Si inzia con una nutrita sezione dedicata ai test hardware: CPU, controller ATA e SATA, RAM; continuando troviamo diversi strumenti per eseguire stress test e benchmark dei componenti del PC. Inoltre sono presenti numerosi programmi di identificazione dell'hardware. Per quanto riguarda i dischi rigidi, troviamo una serie di tool per il controllo dello stato di salute dei dischi (SMART), per la formattazione a basso livello e per

Parted Magic è un'ottima distribuzione su Live CD e Pendrive che può "salvarvi la vita" in più di un'occasione.

CloneZilla è disponibile in numerose distribuzioni e anche stand alone.

il setting delle impostazioni (prestazioni, rumorosità, NCQ, AAM e così via). Troviamo inoltre alcuni file manager che ci consentono di vedere il contenuto dei dischi e copiarlo o spostarlo dove ci fa comodo. Ci sono anche tool specifici per la clonazione dei dischi e la gestione delle partizioni, alcuni dischi di avvio DOS, e molte altre utility dedicate al boot di sistemi problematici, alla gestione del BIOS e molto altro. Insomma, un vero e proprio "coltellino svizzero" del PC.

:: Alternative

In rete si trovano altri live CD dedicati alle emergenze o a compiti specifici, per esempio System Rescue CD (www.sysresccd.org), molto simile a Parted Magic nelle funzionalità e nei programmi disponibili. Degna di menzione la presenza di ClamAV come antivirus: è utile nella "pulizia" di un sistema infetto ostico da ripristinare. Per una lista più esauriente vi consigliamo di visitare www.livecdlist.com, che cerca di elencare tutti i sistemi Live CD esistenti. Dalla colonna "Purpose", potete filtrare i risultati e quindi visualizzare solo le distribuzioni Live che interessano, per tipologia: Rescue e System Administration sono le categorie che riguardano il recupero dati, la clonazione e in genere i compiti amministrativi, mentre le altre categorie sono abbastanza autoesplicative (Desktop, Media Production e così via) da non richiedere ulteriori spiegazioni. Ora serve solo una buona scorta di CD vergini e un po' di tempo!

MeksOne

Fare una radio online? Di successo? Come nasce una Radio 2.0

La storia è semplice e conosciuta. All'inizio degli anni '70, vuoi che molte frequenze radio non erano occupate da nessuno, vuoi che la gente aveva bisogno di farsi sentire e di ascoltare quello che gli piaceva, nascono le prime radio libere/pirata. All'epoca bastava un trasmettitore di sufficiente potenza (alcuni erano eredità del periodo bellico, altri costruiti in maniera artigianale) e poi microfoni, giradischi, una stanza e ovviamente tanta musica ed entusiasmo. Nulla di commerciale, quindi. Semplicemente voglia di divertirsi e di mettersi alla prova. Pensate che all'epoca nella banda FM da 87,6 a 99,9 MHz trasmetteva la Rai e per il resto tutte le frequenze erano libere in particolare da 104 a 108 MHz. Nel 1976 la Legge Mammì pone fine ai sogni di chi faceva radio congelando la situazione e impedendo a nuovi soggetti di entrare nella radiofonia.

:: Déjà vu

Così oggi, a più di trent'anni di distanza dalla nascita delle prime radio libere, troviamo una situazione totalmente diversa nei fatti ma molto simile nelle possibilità. Oggi per aprire una radio FM bisogna acquistare delle frequenze da qualche altra emittente o acquisirne una sull'orlo del fallimento. Sono, tuttavia, operazioni molto complesse, che hanno bisogno di ingenti capitali. La soluzione però è nella rete. Oggi, grazie a Internet, chiunque può essere in grado di 'fare radio' usando strumenti

Il gruppo di FB di RadioFLO è un sistema per catturare nuovi ascoltatori, mezzo pubblicitario e strumento di comunicazione.

e costi alla portata di tutti. Se negli anni '70 era il wattaggio del trasmettitore a definire il raggio d'azione della radio, oggi la rete estende la possibilità di trasmettere a tutto il pianeta. Ma da dove si parte per creare una web radio? Intanto serve uno spazio web, acquistabile da un qualsiasi operatore web o anche utilizzabile a costo zero da siti come Altervista. Questa sarà la vetrina, il luogo dove in pochi clic è possibile creare una pagina web che ospiterà la radio. Il passo successivo sarà noleggiare un server e anche qui internet offre infinite possibilità. Con poche decine di euro al mese avremo un server che farà da collegamento tra noi che trasmettiamo e chi ascolta. A questo punto ci occorre un piccolo software che permetterà al nostro pc di collegarsi al server e trasmettere nel web. Oltre a software specifici (il più famoso dei quali è SAM Broadcaster)

VIA IL VECCHIUME!

Pubblichiamo una storia piccola ma importante: quella di RadioFLO è un'avventura che abbiamo voluto far raccontare da uno dei suoi protagonisti perché è l'esempio di come, grazie alla tecnologia che usiamo tutti i giorni, un gruppo di persone con un'idea vincente possa fare cose straordinarie. Una storia hacker, nel senso più ampio e completo del termine: come usare una serie di tecnologie indipendenti per mettere in pratica un'idea. Una storia che ci riguarda perché l'uso di tecnologie a basso costo, mescolato con sapiente passione, conoscenza dei mezzi e sfruttamento delle mode (social network in primis) ha permesso di realizzare qualcosa apparentemente incredibile: la concorrenza ai big di un mercato, quello radiofonico, in cui i piccoli "tradizionali" sono destinati a subire ed a scomparire.

vi sono anche dei plug-in (uno fra tutti SHOUTcast) che trasformano rapidamente il vostro player musicale in una stazione radio. Ultimi passaggi sono un microfono (ne trovate in giro per tutte le tasche) e ovviamente tanta musica. In ultima nota non dimenticate che tutto va fatto nella legalità e quindi è necessario avere una licenza SIAE ed essere in regola altrimenti si rischiano sanzioni più o meno pesanti.

:: Nasce RadioFLO

RadioFLO è nata nel dicembre 2008 al tavolino di un bar. Un gruppo di amici con la passione per la radio discuteva di come mettere in pratica tutte le idee che venivano fuori tra una birra e l'altra. Un mese dopo nasce materialmente la radio sul web. Gli strumenti sono più o meno quelli elencati sopra, non c'è pubblicità (quindi nessun intento commerciale) e fin dai primi giorni c'è stata la voglia di coinvolgere sempre più gente sia come speaker (in questo caso FLOkers) che come ascoltatori. Se nei primissimi mesi RadioFLO contava una programmazione frammentata e un'organizzazione molto semplice, a distanza di quasi un anno ha collezionato 35.000 visite sul sito e più di 1.600 iscritti al gruppo su Facebook. Sul sito www.radioflo.it trovate il player in flash per ascoltare la radio, una chat per interagire in diretta con i Flokers, una finestra che all'occorrenza diventa webcam e soprattutto un palinsesto che 7 giorni su 7 trasmette musica varia e programmi mirati. RadioFLO non ha una sede fissa e questo la rende molto particolare. I Flokers si passano la linea di programma in programma semplicemente collegandosi/scollegandosi al server e comunicando attraverso community di messaggistica istantanea (come MSN Messenger). Avendo bisogno solamente di una linea Adsl, RadioFLO trasmette anche in diretta da luoghi sempre diversi, diventando quasi una radio 'on the road,' che non aspetta l'ascoltatore ma lo insegue e lo accompagna. Nel corso dei mesi la radio ha organizzato diverse feste (RadioFLO Party) ed era sempre presente dove c'erano musica e divertimento. I Flokers, oggi, sono circa in venti e vengono da varie parti d'Italia, con quasi un Floker per ogni regione, senza contare anche alcune trasmissioni in diretta dall'Estero. Come già detto non c'è nulla di commerciale nel progetto ed è tutto autofinanziato e a basso costo.

Il sito www.radioflo.it riporta palinsesto, strumenti di connessione con i DJ, informazioni: è un elemento indispensabile alla radio.

Aggiornare il palinsesto con un tweet non è folle: è dovuto. Una cosa che le radio tradizionali faticano a comprendere.

:: Tocca a te!

Come vedete, grazie alle possibilità che offre Internet, è semplice creare e gestire una web radio. Quello però che molti sottovalutano è riuscire a formare un gruppo di persone che ci mettono la stessa passione e lo stesso entusiasmo nel seguire un progetto comune. È ovvio che i confini tra 'chi trasmette' e 'chi ascolta' sono molto labili ed è successo a RadioFLO che degli ascoltatori divenissero Flokers. Ciò non significa certo che una radio come RadioFLO sia fatta solo dagli amici e per gli amici perché, se una cosa funziona, il giro cresce e la gente aumenta: sia gli ascoltatori che gli speakers. Non bisogna quindi dimenticare che sono le persone, e la loro passione, che fanno la radio. Sperando di avervi incuriosito, vi aspettiamo sul nostro sito. Buon divertimento e buon ascolto!

PaoloBi

Cifriamo le email

Firmiamo e nascondiamo il contenuto delle email che inviamo utilizzando due noti mail client per Linux

Le email che scambiamo con i nostri conoscenti sono trasferite così come vengono scritte, in chiaro. Nel passaggio dal mittente al destinatario e da un server di posta all'altro, quindi, possono venire intercettate da estranei: ciò, chiaramente, può pregiudicare notevolmente la riservatezza delle informazioni private che diffondiamo o riceviamo. Per proteggere la nostra posta elettronica, quindi, possiamo far uso di un sistema di cifratura come il diffuso e solido standard OpenPGP.

:: Il funzionamento di OpenPGP

Questo sistema di cifratura è basato sulla generazione e lo scambio di chiavi: ciascun utente crea una propria coppia di chiavi di cifratura, la chiave privata e la chiave pubblica; quindi ogni utente custodisce la chiave privata, non rivelandola ad alcuna altra persona, e diffonde il più possibile la chiave pubblica. Ogni chiave pubblica corrisponde ad una ed una sola chiave privata. Sarà appunto la coincidenza tra una determinata chiave pubblica ed una singola chiave privata a permette di cifrare il contenuto delle nostre email, consentendone la lettura solo al rispettivo destinatario. Sfruttando il medesimo principio, poi, sarà possibile "firmare" una email in modo tale che sia ragionevolmente certo che ad averla scritta siamo stati noi e non qualcun altro.

:: GnuPG e Linux

Per proteggere le nostre email utilizzeremo GnuPG (http://www.gnupg.

org), un software open source che segue lo standard OpenPGP, e lo installeremo su un sistema GNU/Linux. Quindi creeremo le chiavi di cifratura ed aggiungeremo le chiavi dei nostri conoscenti usando direttamente la linea di comando; fatto ciò, firmeremo e cifreremo le email all'interno di Evolution (projects.gnome.org/evolution) e KMail (userbase.kde.org/KMail), due potenti mail client grafici per Linux. Faremo così la conoscenza degli strumenti "universali" per gestire le chiavi di cifratura dal terminale, senza per questo rinunciare a delle comode e pratiche interfacce grafiche. Per i nostri esempi, adotteremo come distro di riferimento Ubuntu e Kubuntu 9.04.

Iniziamo dunque assicurandoci di avere installato nel sistema GnuPG. Apriamo una finestra di terminale: su Ubuntu entriamo nel menu Applicazioni e clicchiamo su Accessori > Terminale mentre su Kubuntu clicchiamo sul menu K in basso e selezionamo Applicazioni > Sistema > Terminale. Tramite il terminale dovremo lanciare il comando "sudo apt-get install gnupg".
Poi creiamo le nostre chiavi eseguendo nel terminale "gpg --gen-key". Ci verrà chiesto quale tipo di chiave vogliamo: digitiamo 1 e battiamo Invio per scegliere il tipo "DSA ed Elgamal".

:: Le informazioni personali

A questo punto, premiamo Invio per selezionare la dimensioni di default della chiave (2048 bit) e battiamo di nuovo Invio per indicare che vogliamo una chiave senza scadenza. Confermiamo quanto inserito finora premendo "s" e Invio. Poi inseriamo il nostro nome e cognome e, quindi, digitiamo l'indirizzo di mail a cui vogliamo legare le chiavi che stiamo generando.

Alla richiesta di inserire un commento premiamo Invio in tutta tranquillità. Per confermare tutte le informazioni fornite premiamo "o" e Invio, quindi inseriamo e confermiamo una passphrase, cioè una password lunga che proteggerà la nostra chiave privata.

Adesso verrà creata la coppia di chiavi: per facilitare la generazione di numeri casuali muoviamo il mouse e premiamo tasti a caso sulla tastiera.

Al termine dell'operazione, dopo un certo tempo, ci verrà mostrato l'identificativo (ID) della chiave (nel nostro esempio l'ID è E3812F78). Successivamente, per conoscere l'ID della nostra chiave possiamo eseguire il comando interno di GnuPG che visualizza le chiavi private in nostre possesso, "gpg --list-secret-keys".

```
File  Modifica  Visualizza  Terminale  Aiuto
ale@pitagora:~$ gpg --gen-key
gpg (GnuPG) 1.4.9; Copyright (C) 2008 Free Software Fou
This is free software: you are free to change and redis
There is NO WARRANTY, to the extent permitted by law.

Selezionare il tipo di chiave desiderato:
   (1) DSA ed Elgamal (predefinito)
   (2) DSA (solo firma)
   (5) RSA (solo firma)
Selezione? 1
```

Creiamo le nostre chiavi di cifratura lanciando il comando gpg dal terminale. La prima domanda a cui dobbiamo rispondere riguarda il tipo di chiave desiderata.

I CERTIFICATI DI REVOCA

Può succedere che la propria chiave privata venga persa o conosciuta da altri e risulti, quindi, compromessa. Prevedendo casi simili, al momento della generazione delle chiavi possiamo creare un certificato di revoca: questo consente, appunto, di revocare la nostra chiave pubblica in modo tale che non venga più considerata attendibile da altri. Per creare un certificato di revoca eseguiamo il comando "gpg --output revoca.asc --gen-revoke ID". Persa o compromessa la chiave, quindi, per rendere pubblica la revoca eseguiamo prima il comando "gpg --import revoca.asc" e poi "gpg --send-keys ID".

:: Esportiamo ed importiamo le chiavi

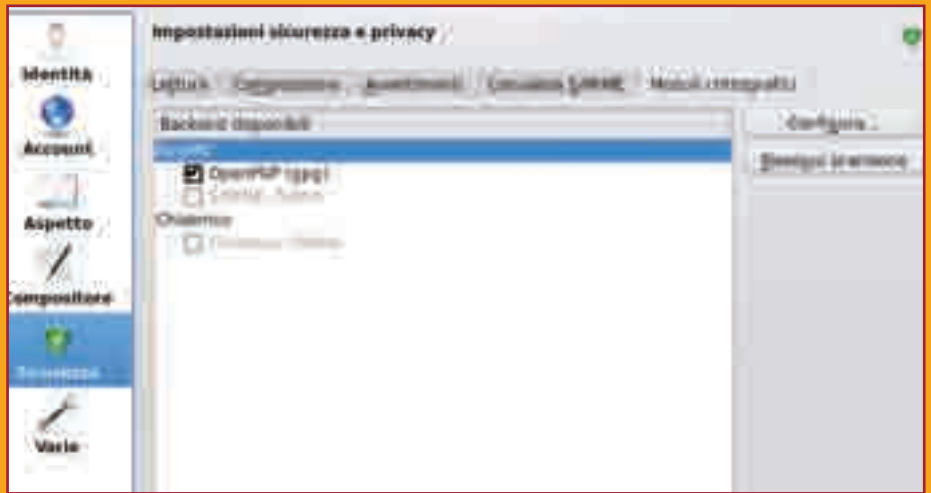
Ora che le chiavi sono state create, non ci resta che diffondere la nostra chiave pubblica. Un modo efficiente per farlo è quello di inviarla ad un key server, cioè un server che archivia le chiavi PGP. Le chiavi inserite in un singolo key server vengono poi, nella gran parte dei casi, propagate negli altri server. Inseriamo dunque la nostra chiave nel key server di default con il comando seguente (sostituiamo ID con l'ID della nostra chiave):

gpg --send-keys ID

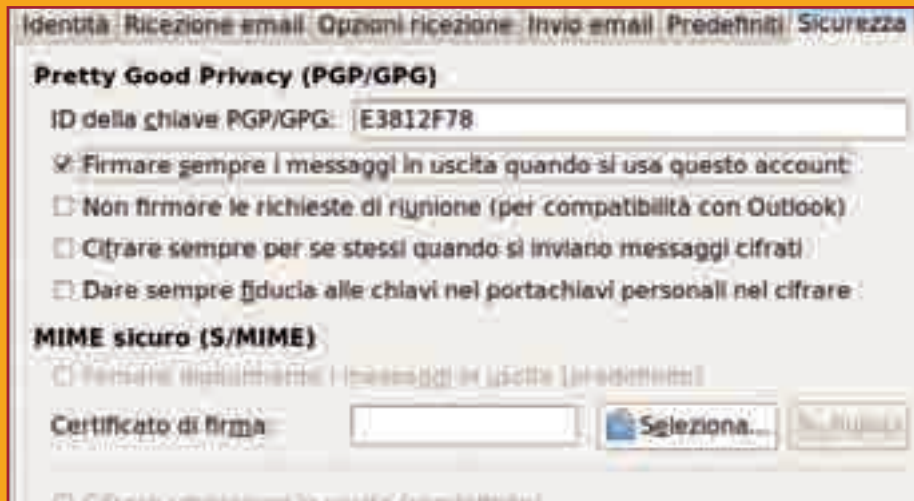
Il passo successivo è importare le chiavi dei nostri conoscenti. Anche qui, possiamo avvalerci di un key server e cercare lì i nostri contatti. Per effettuare ricerche in un key server, lanciamo nel terminale il comando "gpg --search-keys 'email@contatto.it'", inserendo al posto di email@contatto.it l'effettivo indirizzo email del nostro contatto o il nome di questo. Solitamente, verranno trovate più chiavi per un medesimo criterio

di ricerca: digitiamo il numero della chiave che ci interessa per importarla. Avendo a disposizione la chiave pubblica di un nostro contatto, quindi, potremo spedire delle email cifrate e leggibili solo dal contatto stesso. Controlliamo le chiavi lanciando il comando “gpg --list-public-keys”.

:: Email cifrate in Evolution

La configurazione di base di GnuPG, a questo punto, è terminata. Possiamo quindi occuparci dell'integrazione con Evolution, il mail client di default su Gnome. Avviamo il programma, entriamo nel menu Modifica e selezioniamo la voce Preferenze. Nella finestra Preferenze entriamo nella sezione Account di posta, selezioniamo l'account su cui vogliamo attivare PGP (solitamente, l'account di default) e clicchiamo sul pulsante Modica. Nella finestra che appare entriamo nella linguetta Sicurezza. Qui inseriamo come valore dell'opzione “ID della chiave PGP/GPG” l'ID della nostra chiave. All'interno della linguetta Sicurezza possiamo attivare alcune opzioni. Ad esempio, mettendo la spunta su “Firmare sempre i messaggi in uscita” inseriremo automaticamente la nostra firma PGP in ogni email che spediremo. Clicchiamo su OK e poi su Chiudi. Quando creiamo un nuovo messaggo o rispondiamo ad un'email, quindi, nella finestra di composizione possiamo gestire le funzioni PGP entrando nel menu Sicurezza: qui mettiamo la spunta sulle voci “Firma con PGP” e “Cifra con PGP” per, rispettivamente, inserire la nostra firma e per cifrare il messaggio corrente con la chiave pubblica del destinatario.

Anche configurare KMail per gestire firma e cifratura della posta è un'operazione elementare. Tutta la configurazione avviene tramite delle semplici finestre.

:: KMail e PGP

Per configurare KMail in modo da utilizzare le chiavi PGP create, lanciamo il programma e nel menu Impostazioni clicchiamo sulla voce “Configura KMail”. Nella finestra che appare entriamo nella sezione Sicurezza. Qui selezioniamo la linguetta “Moduli crittografici” ed assicuriamoci che l'opzione “OpenPGP (gpg)” sia selezionata. Se vogliamo firmare automaticamente le email che scriviamo, quindi, spostiamoci nella linguetta Composizione della sezione Sicurezza e mettiamo la spunta su “Firma automaticamente i messaggi”. Poi usciamo dalla sezione Sicurezza ed entriamo in Identità: evidenziamo la nostra identità principale e clicchiamo sul pulsante Modifica. Nella finestra Modifica identità entriamo nella linguetta Crittografia e scegliamo come chiave di firma e cifratura la nostra chiave: per fare questo, clicchiamo sui pulsanti Cambia relativi alle due opzioni “Chiave di firma OpenPGP” e “Chiave di cifratura OpenPGP” e, nella finestra che appare, selezioniamo nell'elenco l'ID della nostra chiave e clicchiamo su OK. Tornati alla finestra Modifica identità scegliamo “OpenPGP/Mime” come valore dell'opzione “Formato crittografico del messaggio predefinito”. Per terminare la configurazione clicchiamo su OK in basso. A questo punto, nella finestra principale di KMail clicchiamo sull'icona Nuovo per comporre un nuovo messaggio. Nella finestra Compositore, quindi, clicchiamo su Firma in alto per attivare e disattivare la firma PGP sull'email corrente e su Cifra per abilitare o disabilitare la criptazione del messaggio.

Configuriamo Evolution, il programma di posta di default su Gnome, per firmare automaticamente le nostre email utilizzando la chiave PGP creata in precedenza.

Alessandro Di Nicola

Insuccessi dell'IT

Sempre più in basso!

Le vie del successo sono sempre in costruzione. Spesso sono fatte anche di fallimenti. Per constatarlo basta rivisitare alcune tappe significative della storia dell'informatica.

Possiamo iniziare la nostra panoramica partendo da Casa Microsoft. Dopo il grande successo di Windows 95 che ha completamente riprogettato il modo in cui si poteva usare un computer che non funzionasse con sistema operativo Apple Macintosh, Microsoft ha fatto almeno un paio di tonfi. Quasi a pari merito, possiamo citare Millennium e Vista. Durati sulla scena lo stretto necessario per mettere a punto un nuovo sistema stabile (che, nell'ordine, erano Windows 98 e Windows 7), sono spariti dagli scaffali dei negozi e dai computer a tempo di record. Altre piattaforme non sono sfuggite a brutti scivoloni, come NeXT, l'azienda fondata da Steve Job. NeXTSTEP, uscito nel 1989, ispirò molti programmi Linux e precorse Mac OS X ma nient'altro. Non possiamo non citare BeOS, dei primi anni '90 e che non è mai riuscito davvero a decollare. Vedremo se Haiku, la reincarnazione di BeOS in salsa open source, riuscirà a fare di meglio. Necessaria la citazione di WordPerfect: un eccezionale elaboratore di testi prodotto da Satellite Software che venne venduto a Novell, poi a Corel e sparire nell'assoluto nulla.

:: Buchi nell'acqua

Anche Apple può vantare un buon numero di insuccessi, uno per tutti: l'Apple Lisa. Annunciato nel 1983 fu un disastro assoluto per Apple, con un costo (10.000 dollari) decisamente scoraggiante.
In campo server di rete, il Cobalt Qube prometteva grandi cose quando è stato presentato al mercato, con una sportiva scocca azzurra, un disco da 8,4 gigabyte e ben 64 megabyte di RAM. Funzionava con una versione modificata di Red Hat Linux e con un'interfaccia grafica su misura. L'acquisto di Cobalt Networks da parte di Sun non è bastato a salvare il Cobalt Qube dall'estinzione.
Cambiando completamente area, possiamo passare all'IPv6, successore dell'IPv4. La rete potrebbe restare improvvisamente senza indirizzi IP liberi e non è ancora stata trovata una soluzione definitiva al problema, ma il problema rivelerà le sue apocalittiche conseguenze quando verrà assegnato l'ultimo indirizzo IPv4 e sembra proprio che l'IPv6 non sarà la cura. A proposito di reti e affini, è necessario parlare delle cosiddette Reti mesh. Una "rete a maglie" basata su reti locali senza fili, cooperativa, che prometteva di portare Internet ovunque. Idea strepitosa ma fallita per i troppi interessi (economici)contrari. Può sembrare strano aggiungere il formato MP3 a questa lista: uno dei formati di file più rivoluzionari della storia informatica ma con problemi legati alle licenze che gli hanno reso impervio il cammino verso il successo. Come non concludere con il bug del 2000? Un premio dovuto all'inutile catastrofismo perché non è successo assolutamente nulla: le banche non hanno perso i nostri soldi, la sicurezza mondiale non ha subito colpi e tutti ci siamo limitati a farci gli auguri.

Bartolomeo Gavi

Uno dei più efficaci sistemi crittografici cade sotto i colpi del brute force... Per merito di una "nuvola"

Anche il PGP è BATTUTO

Ok, una nuvola ispira tutto tranne violenza, o la capacità di infliggere dei danni a qualcuno o qualcosa. Eppure c'entra, eccome se c'entra, con la sconfitta del PGP. Proprio lui: nato come programma a sé stante, per opera dello sviluppatore Phil Zimmermann, il Pretty Good Privacy ha rivestito un ruolo sempre più importante. Fino alla consacrazione, quando il noto Bruce Schneier, nel suo seminale "Applied Cryptography", lo definì come il modo per arrivare "probabilmente il più vicino alla crittografia di livello militare". Mica poco, vero? Il segreto del PGP sta nella crittografia asimmetrica che utilizza, detta "a chiave pubblica" (anche se supporta pure quella simmetrica). In pratica, il destinatario del messaggio genera due chiavi: una pubblica, che serve per codificare l'informazione, e una privata, che serve al destinatario per decodificare il contenuto. Una spiegazione ingiustamente breve e casereccia, ma che riassume un'efficienza raramente eguagliata nel mondo della crittografia moderna. Questo ha fatto in modo che PGP sia oggi ampiamente sfruttato per le comunicazioni che necessitano di protezione, in qualsiasi ambito.

:: Forza bru(t)ta?

Fino ad oggi, il PGP si è goduto la sua fama, seduto comodamente sugli allori. Insomma, nessuno è riuscito a batterlo.

In linea MOLTO teorica l'algoritmo sarebbe vulnerabile ad attacchi di forza bruta ("brute force"), effettuati generando sequenze di combinazioni alfanumeriche fino a trovare la corretta chiave crittografica. Peccato che non esistano elaboratori o reti di elaboratori in grado di riuscire nell'impresa in tempi ragionevoli: nella migliore delle ipotesi servirebbero parecchi anni per trovare una sola chiave. Si dice che perfino l'impenetrabile NSA (National Security Agency), l'agenzia dedicata alla sicurezza digitale degli Stati Uniti, non sia in grado di violare il PGP. La conferma arriverebbe dal fatto che lo stesso Zimmermann, nel Febbraio 1993, per via della sua scoperta,

fu indagato con l'accusa di esportazione di armi senza apposita licenza. Ciò paragonava le chiavi a più di 128 bit usate dal sistema PGP a vere e proprie munizioni di guerra.

:: Ci provò Elcomsoft

Evidenziata una volta di più la potenza del PGP e ricordata la sua ampia diffusione, arriva la doccia fredda: il PGP è stato crackato. Un crack vero, che nulla ha a che fare con quello, tanto paventato ma ancora tutto da verificare, annunciato da Elcomsoft (www.elcomsoft.com) circa un anno fa. Il loro software Distributed Password Recovery, correzione dopo correzione, è arrivato a eseguire attacchi di forza bruta su semplici chiavi PGP di file ZIP ma si parla comunque di attese di almeno 2000 giorni. Questo malgrado il programma di Elcomsoft si faccia forte di una struttura in grado di appoggiarsi a sistemi fino a 64 CPU, con la capacità di sfruttare fino a 32 processori grafici (GPU). Eppure, dati alla mano, tutto questo non bastava. Così, oggi, ecco la nuvola.

Philip Zimmermann, philzimmermann.com, creatore di PGP. Inutile dire che, in questo periodo, sorride molto meno...

Elcomsoft, www.elcomsoft.com, ha creato un sistema di brute force per il crack di file protetti da PGP ma risulta estremamente lento. Nella cloud diventa una scheggia!

:: Una nuvola carica di...

Ci riferiamo ovviamente a un sistema di "cloud computing", in grado di demandare i calcoli più complessi a intere sale server pronte all'uso. Si tratta di una delle tecnologie più chiacchierate degli ultimi tempi e sono già molti i colossi del settore informatico che la stanno utilizzando. Tra questi Amazon, il più grande negozio online del mondo, che col suo Amazon Elastic Compute Cloud (detto "Amazon EC2") ha dimostrato di essere un passo avanti anche nel settore del "cloud". Di base, EC2 è un servizio a pagamento (i prezzi partono da circa 0,0634 euro per ora d'utilizzo) che offre un'infrastruttura pronta all'uso, a cui dare in pasto i più svariati tipi di elaborazione tramite web. Detto questo, ecco l'idea geniale: visto che, ironia a parte, la strada percorsa da Elcomsoft e il supporto multi-processore era quella giusta e visto che EC2 consente di accedere a una potenza di molto superiore a quella di 64 CPU e 32 GPU, perché non unire le due cose?

:: Amazon ti aiuta

Se lo sono chiesti anche i ragazzi di Electrical Alchemy, che hanno lavorato duramente a una tecnologia che unisca il Distributed Password Recovery e l'EC2 di Amazon. Insomma: il concetto è quello di utilizzare il software di Elcomsoft, demandando però i calcoli non a una rete locale ma ai server cloud della compagnia di Jeff Bezos. In realtà non si è trattato di una passeggiata, per via di alcuni aspetti critici di natura tecnica. Per prima cosa, i nostri intrepidi eroi si sono dotati di una Amazon Machine Image (AMI) a 32 bit, visto che il programma di Elcomsoft non è disponibile in una più evoluta versione a 64 bit. Fatto questo, hanno utilizzato la API di EC2 per lanciare un'apposita istanza e passare, quindi, alla configurazione del programma Distributed Password Recovery (o "DPR"). Data la struttura del programma di decrittazione, i ragazzi di Electronic Alchemy (o "EA") hanno scaricato e installato la versione "agent" di DPR. Questo per gestire il programma di-

rettamente dai loro computer e lasciare al cloud l'unico compito di effettuare i calcoli necessari. Una volta installato l'agent di DPR, questo è stato avviato, configurandolo con l'inserimento di un apposito IP pubblico e ponendo a NULL la chiave

HKEY_LOCAL_MACHINE\Software\ElcomSoft\Distributed Agent\UID

Una volta configurato di tutto punto il programma di Elcomsoft, i ragazzi "alchemici" hanno installato l'EC2 AMI Tool, col quale collegare EC2 e Distributed Password Recovery. Registrate e avviate le istanze, si è quindi passati alla configurazione del DPR Manager, con relativa assegnazione del compito da svolgere.

La nuvola di Amazon, aws.amazon.com/ec2, ha una gestione Web based. Unita a un sistema di Elcomsoft, modificato, permette risultati di decifratura sbalorditivi.

:: Prova riuscita!

Per l'occasione, quelli di Electronic Alchemy hanno organizzato un attacco di forza bruta considerando lettere maiuscole, lettere minuscole e numeri da 0 a 9, con una lunghezza della chiave tra 1 e 8 caratteri. Il tutto contro, guarda caso, un file ZIP protetto con PGP, e sfruttando l'offerta più economica di EC2 (quella più lenta). Il risultato? Appena 500 chiavi generate e provate al secondo, per un totale stimato in circa 10 anni. Incassata questa (mezza) sconfitta, i nostri eroi sono tornati al lavoro e… al salvadanaio, optando per una soluzione EC2 più veloce. Il guadagno in velocità è stato enorme, scendendo ad appena 122 giorni di elaborazione. A questo punto, il sistema EC2 era stato spremuto a dovere, tanto che Amazon non disponeva di soluzioni più veloci. Questo per via del timore che dei malintenzionati usino EC2 per creare degli attacchi Denial of Service (DoS). Così i ragazzi hanno messo giù qualche riga di codice Python, aggirando il limite e aumentando ulteriormente la velocità di elaborazione. Così, con qualche trick, si è passati a tempistiche nell'ordine di qualche giorno. Non male, per un sistema di protezione nato per richiedere anni e anni di calcoli!

PGP è distribuito in varie versioni: quella internazionale, liberamente utilizzabile, si trova all'indirizzo www.pgpi.org. Ormai, però, non è più tanto sicura…

::Fine di un'epoca

La tecnologia messa a punto da Electronic Alchemy è ancora in fase di sviluppo e perfezionamento ma è certo che la strada intrapresa verso la decrittazione in tempo reale sia quella giusta. La nascita delle tecnologie cloud e della loro disponibilità di potenza di calcolo non era ovviamente prevista da Zimmermann. Ora non ci resta che seguire questi formidabili ragazzi nelle loro peripezie, grazie al sito ufficiale www.electricalchemy.net. Che la nuvola sia con loro.

Riccardo Meggiato

Immagini SPIA

Basta un nulla per alimentare lo spam che riceviamo

L'uso diffuso delle mail in formato HTML ha certamente aumentato le possibilità di comunicazione, trasformando un mero strumento in qualcosa di gradevole sia per le aziende che per i comuni utenti. L'introduzione di elementi grafici in un ambito di Rete, tuttavia, espone il fruitore a rischi legati al download delle immagini da siti Web. Immaginiamo, per esempio, di creare una mail che contenga in basso un'immagine derivata da una pagina dinamica, nel formato: . La pagina chiamata img.php non ha altro scopo che fornire come risultato un'immagine, così da permetterne il download e l'incorporazione nella mail. Il meccanismo è legittimo e si presta, per esempio, a creare una pagina che possa gestire ogni immagine di un sito o di mail HTML: il codice indicato dopo la variabile id potrebbe benissimo essere usato per indicare l'immagine da fornire. Pensiamo, invece, che la pagina fornisca sempre la stessa immagine e che ogni codice, univoco, sia associato a un indirizzo di posta elettronica. All'apertura della mail HTML, il programma recupera l'immagine. Questa viene composta dalla pagina PHP che rileva la variabile passata ed è in grado di confermare sia la validità dell'indirizzo di posta a cui è stato spedito il messaggio che la sua apertura. Il meccanismo, ovviamente, non si ferma qui perché la semplice fornitura di un elemento permette al demone http di ottenere una serie di altre informazioni, grazie alle variabili lato server. Così facendo, la nostra pagina img.php può anche scoprire la locazione geografica del lettore della mail, grazie a una operazione di geo ip location, il sistema operativo usato, l'ora precisa della lettura. È possibile, persino, la lettura e scrittura di cookies: da questo deriva, nel caso di siti con registrazione, identificare l'utente

:: Web bug

Immaginiamoci di prendere la nostra immagine di 40x40 pixel e di trasformarla in un'immagine 1X1. Pensiamo, addirittura, di renderla trasparente, di metterla nascosta all'interno della mail HTML. Abbiamo creato un Web Bug, conosciuto anche come Web Beacon o Tracking Pixel: un singolo punto invisibile in una mail HTML che fornisce informazioni vitali a chi ce l'ha inviata. Lo scopo di questa operazione è banale: avere la certezza di trattare con persone reali. L'applicazione di questa tecnica è addirittura scontata: uno spammer può, con un accorgimento tutto sommato banale, ripulire il suo database dagli indirizzi "a perdere" e valorizzare quelli validi, così da ottenere un target certo. La cosa diventa ancora più importante quando si associano diversi codici univoci allo stesso indirizzo, usandoli per mail su temi diversi. Lo spammer potrebbe, per esempio, inviare 3 mail allo stesso indirizzo, con provenienze diverse, promettendo facili guadagni, l'acquisto di medicinali e l'acquisto di software contraffatto. La validità dell'indirizzo della vittima è assicurata se almeno uno dei tre codici viene chiamato in causa dal meccanismo ma c'è di più: a seconda del codice rilevato, lo spammer può rendersi conto se, con quel corrispondente particolare, conviene di più insistere su certi argomenti piuttosto che su altri. Il risultato è una vera e propria profilazione delle vittime che, al limite del social engineering, permette di condurre degli attacchi mirati: decisamente molto più efficaci rispetto a un banale (e inutile) bombardamento a tappeto.

Un RSS Feed può contenere immagini. Quindi può contenere anche uno o più web beacon. Facciamo attenzione.

SSL bucato

Sono a rischio tutte le transazioni cifrate su Internet, pari a svariati milioni di dollari. Tra queste, ovviamente, tutti i nostri conti bancari online!

Lo scorso agosto degli analisti hanno scoperto una grave falla di sicurezza che affligge il protocollo SSL. Le transazioni criptate sono oramai la base di comunicazioni interbancarie e rilascio di certificati di sicurezza per l'accesso ad aree protette per servizi evoluti, ma anche la gestione della posta privata. Segue che l'argomento ha avuto subito un'eco notevole.

:: La falla

Il nome che è stato scelto per definire la falla è SSL/TLS Authentication Gap e riguarda l'autenticazione dell'utente. L'attaccante, tramite l'inserimento di codice malevolo, può sostituirsi all'utente reale con un classico attacco "man-in-the-middle" e risultare correttamente autenticato nella comunicazione SSL. La vulnerabilità sfruttata in questo attacco invalida parzialmente il lucchetto SSL sul quale si basa la verifica di sicurezza della comunicazione con un sito web, lo stesso che viene indicato nei moderni browser proprio per garantire la sicurezza.

Gli scopritori Marsh Ray e Steve Dispensa, dipendenti di PhoneFactor (un'azienda specializzata in servizi di autenticazione per utenti di reti cellulari), hanno dimostrato l'efficacia della falla a un gruppo di lavoro di cui fanno parte Microsoft, Intel, Nokia, IBM, Cisco, Juniper, Open SSL, Apache, NSS, Red Hat, Leviathan Security Group e rappresentanti della Internet Engineering Task Force (IETF). Durante tale incontro, svoltosi in modo molto riservato a fine settembre, è stato assicurato che la pubblicazione dei documenti relativi all'attacco verranno pubblicati solo agli inizi del prossimo anno, per dar tempo a tutti i soggetti interessati di provvedere in modo opportuno.
Tuttavia già all'inizio di novembre, si è generata una discussione all'interno del gruppo di lavoro di IETF che ha svelato il problema e la notizia si è diffusa rapidamente in tutta la rete. PhoneFactory ha dovuto quindi ammettere che era già stato creato un team al lavoro per chiudere la falla (vedi Advisory al link extendedsubset.com/?p=8)

:: L'attacco

Come è possibile realizzare un attacco di questo tipo? Oltre a doversi frapporre tra client e server si deve interagire con certificati di autenticazione criptati.

Al servizio di quanti si interessano di sicurezza è stato rilasciato SSLsniff, un tool che permette di disturbare proprio il traffico che viene scambiato via SSL creando falsi certificati. In congiunzione a SSLsniff va però intercettato il traffico con ARPspoof per realizzare un attacco man-in-the-middle. ARPspoof convince il pc della vittima che l'attaccante sia il vero router verso il quale inoltrare le richieste, incluse quelle per i certificati SSL. Il pc dell'attaccante riceve le richieste e le inoltra tutte tranne quelle SSL (porta 443). A questo punto SSLsniff riceve le connessioni dal client, realizza una vera connessione verso il server reale e guarda le informazioni nei certificati intercettati.

SSLsniff può poi funzionare in due modalità:

- in Authority Mode è in grado di generare i certificati al volo per qualunque sito si voglia simulare
- in Targeted Mode, accede a una cartella dove sono presenti certificati già pronti per eseguire attacchi mirati nei confronti di specifici client

Per la prima modalità, dopo aver creato un certificato dinamicamente, lo rigira al client che su accettazione diventa vulnerabile. Nella seconda modalità è possibile realizzare attacchi (hijack) come la creazione di falsi update per software come Mozilla Firefox o Thunderbird che gestiscono l'auto-update. Ovviamente l'ambiente più naturale nel quale testare queste applicazioni estreme è linux. Il software viene quindi rilasciato in forma sorgente e andrà prima di tutto compilato. Insieme al codice viene rilasciata una efficace documentazione relativa all'attacco tipico. Non è nostra intenzione mostrare tutti i passi che permettono di realizzarlo e unicamente a scopo didattico descriviamo a livello macro cosa andrebbe fatto:

L'handshake SSL è una delle fasi più critiche delle comunicazioni protette. Può essere intercettato e analizzato tramite tool facilmente reperibili sul Web.

Tutti i conti online sono a rischio: SSL è fondamentale per il loro funzionamento.

- prima di tutto la macchina attaccante deve poter sostituire il router e va attivato il forward IP
- nelle tabelle di routing va aggiunta una regola per intercettare il traffico HTTPS (443)
- vanno poi aggiunte le regole per intercettare tutto il resto del traffico (IMAP, POP3, IRC over SSL, ..)
- "spoofando" il MAC address del router e sovrascrivendo quello della nostra scheda (tramite ARPspoof)

A questo punto tutto il traffico SSL viene rediretto verso la macchina attaccante tramite SSLsniff e registrato automaticamente in un file.

:: Contromisure

Il problema riguarda il protocollo, in particolare il Transport Layer Security (TLS) e non una sua specifica implementazione. Questo equivale a dire che tutti i siti web che utilizzano certificati provenienti da client, inclusi gli utenti che utilizzano chiavi basate su smartcard sono vulnerabili. Di conseguenza la risoluzione non può che essere radicale: nelle librerie SSL deve essere chiusa la falla e tutti i produttori di software che le utilizzano devono aggiornarle prima possibile, così da permettere a ogni utente di aggiornare a sua volta le versioni di software bacate in proprio possesso. Al momento sono stati concordati all'interno del gruppo solo dei metodi per miticare la vulnerabilità, che risulta ancora aperta con codice CERT (VU#120541).

I vendor legati al mercato della sicurezza tendono a minimizzare la falla di sicurezza, spiegando che il tipo di autenticazione messa in crisi è raramente usata. PhoneFactor afferma esattamente il contrario. Nel dubbio, chi fosse interessato può seguire il thread ufficiale dell'IETF (www.ietf.org/mail-archive/web/tls/current/msg03928.html) e tenersi pronto agli aggiornamenti software.

NoeXKuzE

Il sistema Android

L'alternativa open di Google all'iPhone di Apple?

Il progetto Android compie due anni proprio in questi giorni, ma solo di recente si è cominciato a sentirne parlare in modo consistente. L'occasione è, ovviamente, la comparsa sul mercato consumer di telefoni che dispongono del "nuovo" sistema, in diretta concorrenza con i big del settore. In questo periodo Android si è evoluto e ha conquistato non solo l'interesse degli utenti, ma anche quello delle principali aziende legate alla telefonia mobile, mostrando di essere un prodotto su cui vale la pena investire. Per scoprire il motivo di tanto interesse abbiamo deciso di approfondire l'argomento, scoprendo diverse caratteristiche interessanti di questo progetto. Innanzi tutto, Android non è "il telefono di Google": non è (esclusivamente) di Google, nel senso che, pur avendo un forte sostenitore e sviluppatore nell'azienda di Mountain View, il progetto fa capo a un consorzio chiamato Open Handset Alliance, dedicato allo sviluppo di standard aperti per i dispositivi mobili. Google fa parte del consorzio insieme ad altre grandi aziende come ad esempio Motorola, HTC, Intel, Nvidia, Asustek Computer e Vodafone. Android non è neanche un telefono specifico, ma piuttosto un sistema operativo in grado di girare su diversi dispositivi, fra cui telefoni, internet tablet ed ebook reader (en.wikipedia.org/wiki/List_of_Android_devices). Il sistema è rilasciato come open source fino alla penultima versione, la 1.6, sul sito source.android.com, e corre voce che a breve anche la recentissima versione 2.0 sarà distribuita con la medesima licenza. Grazie alla disponibilità del codice, sono disponibili su Internet numerose versioni modificate di Android, che oltre ad offrire un maggiore controllo del sistema forniscono in anteprima nuove funzioni e bugfix.

:: Architettura del sistema

Android è un sistema basato su un kernel Linux, personalizzato per i dispositivi su cui esso deve girare (su questa "personalizzazione" sono presenti in rete anche commenti decisamente negativi, ad esempio su bit.ly/2SjGxJ). Al kernel si appoggiano diverse librerie specifiche, come ad esempio OpenGL per la grafica 3D e SQLite per i database, e una virtual machine sulla quale gira il codice delle applicazioni (e del framework che mette a loro disposizione i servizi principali del sistema, come ad esempio la gestione delle finestre, delle notifiche e della telefonia). La virtual machine, chiamata Dalvik, merita un discorso a parte. Essa, infatti, pur consentendo agli sviluppatori di far girare codice Java su dispositivi Android, non è

L'architettura di Android è composta da diversi strati, partendo dal kernel fino ad arrivare alle applicazioni finali.

una Java Virtual Machine: il bytecode della JVM è incompatibile con Dalvik e, per poter sviluppare su Android, è necessario usare Eclipse con un particolare plugin fornito da Google. Il motivo di tutto ciò è che Dalvik è appositamente ottimizzata per sistemi mobili, con poca memoria e CPU non particolarmente performanti (all'indirizzo www.youtube.com/watch?v=rAxYdfzs3t0 possiamo trovare un video che descrive Android, e Dalvik in particolare, in modo molto dettagliato).

:: Cosa ci posso fare?

Ciò che è possibile fare con un dispositivo Android cambia, naturalmente, a seconda del dispositivo stesso: con un telefono magari sarà complicato leggere libri, mentre con un ebook reader sarà impossibile telefonare! La buona notizia è che recentemente i produttori di telefoni hanno deciso di investire in dispositivi avanzati in grado di sfruttare al massimo Android: gli ultimi cellulari hanno infatti un hardware molto ricco (con fotocamere, gps, bussole e accelerometri), ormai in grado di competere con dispositivi come gli iPhone.

Le funzioni a disposizione della versione più recente di Android sono mostrate in un video all'indirizzo www.android.com: ad esempio, la gestione dei contatti integrata ed estensibile a diverse applicazioni "sociali", un supporto bluetooth avanzatoveramente funzionante (ebbene sì, fino alla versione precedente il bluetooth poteva essere usato per tutto... Tranne trasferire file!), e così via. Oltre a questo ci sono anche tutte le applicazioni incluse di default in Android: Gmail, Google Maps, YouTube e Gtalk consentono di accedere ai corrispondenti servizi dal proprio dispositivo mobile attraverso un'interfaccia ottimizzata; un discreto browser con supporto per javascript e Flash permette di visitare la maggior parte dei siti Web senza problemi; calendario e gestione contatti permettono di avere un'agenda sempre a portata di mano, conservandone però il contenuto direttamente online nel nostro account di Google.

Oltre ai programmi distribuiti insieme ad Android, una grande quantità di applicazioni è disponibile online: per la loro distribuzione Google ha messo a disposizione un canale ufficiale, chiamato Android Market, accessibile sia da browser (www.android.com/market) che direttamente dal telefono; oltre ad esso sono disponibili diversi altri canali, come ad esempio AndAppStore (andappstore.com) e SlideMe (slideme.org). La quantità di applicazioni a disposizione non raggiunge ancora le cifre di iPhone, ma ha già superato le 10000 ed è in costante crescita.

:: Android o iPhone?

Parlando di iPhone, la scelta è ardua e sicuramente (come d'altra parte accade fin dalla notte dei tempi) darà vita a una nuova "guerra fra religioni" nella comunità geek. Volendo sottolineare le differenze principali, Android è un sistema in larga parte aperto, non richiede l'utilizzo di applicazioni o sistemi operativi particolari ne' per funzionare ne' per svilupparci software, consente la distribuzione di programmi attraverso differenti canali e al momento è in fase di crescita, con una popolarità decisamente inferiore rispetto ad iPhone. Quest'ultimo, oltre ad essere più famoso e ad avere molte più applicazioni disponibili, è perlopiù un sistema chiuso e vincola l'utente in diversi modi, sia dal punto di vista software (un solo appstore ufficiale, iTunes indispensabile, SDK solo sotto

Android 2.0 in esecuzione su un emulatore: da notare, immancabile, la barra di ricerca su Google, già integrata!

Mac) che hardware (ad esempio, la batteria non è estraibile). La scelta del sistema più aperto, d'altra parte, non è ovvia: se, da una parte, l'approccio hacker potrebbe preferire ciò che è già condiviso in modo libero, dall'altra è proprio il sistema chiuso quello che necessita di una "liberazione"...

:: Conclusioni

Dire tutto di Android in un solo articolo non è semplice, ma per fortuna, ultimamente, sembra che non si parli di altro: partendo dai link suggeriti all'interno dell'articolo è possibile trovare un sacco di approfondimenti sui temi descritti. Se le informazioni che troviamo su Internet ci fanno venir voglia di comprare un dispositivo Android, è bene che teniamo presente un paio di osservazioni. Per prima cosa, poiché la maggior parte delle applicazioni disponibili fa uso di una connessione dati, sarà bene che controlliamo il costo del piano dati del nostro gestore telefonico. Per finire, visto il periodo dell'anno, rimandando il nostro acquisto a dopo Natale, forse, potremmo riuscire a risparmiare un po' di denaro.

Quali sono le prospettive dell'IT Security nel 2009 ? Lo chiediamo a Michael Boelen!

Due chiacchiere con Michael Boelen

In esclusiva per Hacker Journal vi proponiamo un'intervista a Michael Boelen, autore di due dei più famosi ed utilizzati tool opensource per l'auditing di sistemi UNIX (Rootkit Hunter e Lynis) nonché noto esperto di sicurezza. Buona lettura!

HJ: Ciao Michael, innanzitutto ti ringraziamo per averci dedicato parte del tuo tempo.
M. Boelen: Grazie a voi! Il nome della rivista suona bene e rispecchia esattamente quelli che sono i miei interessi; è quindi per me un piacere rispondere alle vostre domande sottolineando come l'attenzione rivolta ai progetti opensource ed alla sicurezza per i vostri lettori si traduca per me nell'opportunità di mettere questi ultimi a conoscenza del mio lavoro.

HJ: Tanto per cominciare: chi è Michael Boelen e cosa fa nella vita?
M. Boelen: Ho 27 anni e vivo nella zona meridionale dei Paesi Bassi. Lavoro per la Snow BV, una società di consulenza olandese composta da specialisti UNIX con conoscenze in ambito di rete, storage e security. Questi ultimi due campi sono quelli in cui destino parte della mia giornata lavorativa alla Philips, per la quale sono security officer. Oltre al lavoro leggo molti libri per studio e, naturalmente, svago. Molti di questi riguardano la sicurezza; questo probabilmente non vi meraviglierà considerando il mio lavoro. Dopo essere stato dietro ad una scrivania tutto il giorno mi piace, nel tempo libero, praticare jogging ed andare in bicicletta.

HJ: A che età inizia la tua passione per l'informatica? Da quando ti occupi di tematiche connesse all'Open Source e alla sicurezza?
M. Boelen: All'età di circa otto anni feci la mia prima esperienza con un Commodore 64. A quel tempo la gente iniziava a comprare i primi personal computer mentre io giocavo con il mio Commodore (da bravo bimbo). Quando compii 10 anni iniziai ad utilizzare il Basic copiando sorgenti da libri per creare piccoli giochi. Fu proprio questa esperienza ad avviarmi nella programmazione. Feci la mia prima esperienza con software opensource quando ero studente. Installammo linux e constatammo che, dopo molto tempo passato ad utilizzare MS-DOS e Windows, esso si presentava in maniera leggermente "diversa". Allo stesso tempo maturava il mio interesse nelle tematiche connesse alla rete ed alla sicurezza. Questi interessi divennero più forti negli anni successivi.

HJ: Per Michael Boelen la sicurezza è un prodotto o un processo ?
M. Boelen: A mio avviso la sicurezza è entrambe

le cose. Essa diventa un "prodotto" quando si raggiunge un certo grado di fiducia nel fatto che i nostri dati sono al sicuro; d'altra parte è un "processo" in continuo sviluppo nel quale tutti devono partecipare per mantenere gli stessi standard qualitativi in futuro. Possiamo anche fare un paragone utilizzando un prodotto di sicurezza stesso come un IDS. In questo caso hai bisogno di gestire effettivamente il device (= processo) per dare all'IDS il suo valore e renderlo ancora un po' più sicuro (= prodotto).

www.packetstormsecurity.org è un sito che si occupa di tematiche legate alla sicurezza: ospita diverse pagine dedicate a Michael e diverse guide per Lynis.

HJ: Come giudicheresti il mercato legato alla sicurezza negli ultimi 10 anni a questa parte? Dal tuo punto di vista le aziende investono maggiormente in sicurezza rispetto al passato?
M. Boelen: Senza dubbi il mercato che ruota attorno alla sicurezza è in crescita. Risulta ancora scarsa, però, la quantità di figure professionali certificate, mentre la richiesta di queste è sempre maggiore. Con l'introduzione di vari regolamenti ed iniziative come SOx, HIPAA e PCI, sempre più aziende sono tenute a rispettare regole predefinite. Gli stessi clienti esigono che le aziende trattino con maggiore serietà i loro dati finanziari e la loro privacy come mai è stato fatto finora. Inoltre la continua attenzione da parte dei media per queste dinamiche, fa sì che queste siano più consapevoli delle problematiche connesse alla sicurezza, investendo in infrastrutture, processi e persone.

HJ: Secondo te, qual è la percezione che l'utente, definiamolo "medio", nel 2009, ha delle tematiche connesse alla sicurezza informatica?
M. Boelen: Gli utenti generici sono spesso ignoranti circa le dinamiche della sicurezza, malgrado siamo nel 2009. Parte di questi utenti non sa cosa sia un antivirus, come e perché dovrebbero fare una copia di backup dei propri dati e quando evitare di collegarsi ai link ricevuti via e-mail. Non posso neanche dargli colpa dal momento che la sicurezza è ancora argomento nuovo nel mondo in cui viviamo oggi. Un altro problema è che la gente sottovaluta il valore dei loro dati personali. Tutti vogliono avere la raccolta delle foto delle proprie vacanze ma quanti fanno regolarmente un backup di queste ? Speriamo che nei prossimi 10 anni a questa parte la sicurezza sarà parte integrante del mondo informatico in cui viviamo, come Internet lo è ormai per molti di noi.

Boelen è diventato famoso per aver realizzato Lynis: una eccezionale suite per la sicurezza. Informazioni su programma e autore si trovano sul sito www.rootkit.nl.

HJ: Come descrive Michael Boelen la figura dell'hacker moderno?
M. Boelen: Per me l'hacker moderno è sempre lo stesso entusiasta che cerca di scoprire come funzionano specifiche parti della tecnologia in senso vario. Quando si parla dei blackhat la definizione, per me, invece è cambiata. Mentre prima solo persone particolarmente abili riuscivano a far breccia in un sistema informatico, ora

Ispezionare registri, tracciare dati, testare configurazioni: fare hacking non è solo questo.

quasi tutti riescono a farlo con l'ausilio di qualche potente tool.

HJ: É evidente che l'interesse rivolto da parte di istituzioni e media all'opensource è sempre maggiore. Come spieghi questo fenomeno?
M. Boelen: Il software opensource sta diventando maturo, ha sempre più features interessanti ed, usualmente, è disponibile al miglior prezzo possibile per l'utente: gratis. In questi periodi difficili per l'economia, le aziende effettuano tagli al budget e spesso devono cercare alternative alle applicazioni commerciali esistenti. L'attenzione dei media è un grande vantaggio per il software opensource. Penso che l'attenzione da parte dei media e l'opensource traggano benefici vicendevolmente: rivolgendo attenzione a tali software, la gente inizia usarli ed in cambio vuole sapere di più su di essi. Dopotutto molte riviste sono nate per rispondere a questa domanda come molti giornali dedicati a linux.

HJ: Vedere oggigiorno installata una distro Linux non meraviglia più di tanto rispetto a qualche tempo fa. Questo avviene ormai anche in ambito casalingo. Qual è l'approccio che consiglieresti ad una persona che si avvicina per la prima volta al mondo del software Open Source?
M. Boelen: Consiglierei di fare piccoli passi e capire che ci si muove in un nuovo territorio. Il software opensource esiste in tante forme diverse, ma può presentare le sue sfide. Da una parte abbiamo programmi facili da utilizzare, ben documentati e con una grande base di utenza. Dall'altra, abbiamo software che è miseramente documentato e che risulta alquanto impossibile da installarsi. Siate preparati a leggere le pagine dei man(uali), la documentazione o a richiedere qualche aiuto sui forum relativi. Se iniziate a lavorare con software opensource prendetevi il tempo per rispondere alla seguente domanda: "Cosa può fare questo software per me e cosa posso fare per ottenere il massimo da esso?".
Penso sia possibile comparare la scelta di un software opensource all'acquisto di un'automobile nuova: essa avrà sempre un telaio, un motore e quattro porte ma spetta a voi scegliere il colore. A volte dovrete accettare il fatto di non poter scegliere il vostro colore preferito. Ma alla fine scoprirete che ci sono tantissimi tool buoni, spesso con features che non trovereste nemmeno in applicativi commerciali.

HJ: Sappiamo che destini parte del tuo tempo alla realizzazione di software destinati agli "addetti ai lavori", tra questi "Lynis": a chi si rivolge e perchè? Quali sono state le motivazione che ti hanno spinto alla realizzazione di un software simile?
M. Boelen: Lynis può essere descritto come un applicativo per l'auditing di sistemi unix-like. Esso effettua un'analisi del sistema alla ricerca di configurazioni incorrette o vulnerabili. Quest'analisi include i file di default del sistema, il software installato ma anche le patch di sicurezza mancanti. Lynis può aiutare i system administrator a rendere sicuri i loro sistemi, effettuando un duplice controllo sulle loro installazioni di default e confrontando il sistema ad una base di riferimento prestabilita e sicura.
Per i consulenti di sicurezza, l'applicativo può offrire informazioni sul grado di esposizione a vulnerabilità del sistema e se eventuali difetti di configurazione sono stati corretti.
Il principale motivo che mi spinse

alla scrittura di questo software era la totale mancanza di applicativi di questa categoria. Per lavoro devo installare, configurare ed analizzare sistemi. Quando cercavo applicativi per effettuare auditing non trovavo molti tool capaci di offrire una generica analisi del sistema.Un'altra ragione per creare questo tool è quella di migliorare la mia conoscenza dei molteplici aspetti che UNIX ed il software libero ha da offrire. L'ultimo motivo, ma non meno importante, è sicuramente dato dal fatto che sviluppare software opensource offre l'opportunità di essere intervistato!

HJ: Nel tuo sito web, tra i progetti non ancora rilasciati, si annovera "PHPIPS". Possiamo intuire che si tratta di un framework da utilizzare nella scrittura di applicativi web che offre alcune features interessanti come la protezione da attacchi di tipo XSS ed SQL injection. Potresti dirci qualcosa in più? Quando pensi di pubblicare una prima release? In cosa, sostanzialmente, differisce da soluzioni già largamente utilizzate e collaudate in quest'ambito quali "Mod_Security" o le patch e le librerie offerte dal progetto "Hardened-PHP"?

M. Boelen: Questo è corretto.

Un NAS: gestione semplice ma ogni falla di sicurezza può essere catastrofica.

PHPIPS è un framework che serve a bloccare ogni input inaspettato e può essere configurato per filtrare e/o bloccare determinate richieste per ogni singola pagina e tipo di campo (all'interno dei form HTML). La grande differenza in questo momento è che PHPIPS non è ancora disponibile al pubblico, mentre gli altri si.
I due progetti che hai menzionato sono maturi ed hanno i loro specifici punti di forza, mentre PHPIPS è semplicemente un framework.

HJ: Sei l'autore di uno uno dei software più utilizzati e conosciuti nel panorama del free software per l'analisi di sistemi Unix volta alla ricerca di rootkit e software dannoso. Stiamo parlando naturalmente di "Rootkit Hunter". Considerata l'adozione da parte della quasi totalità delle distro linux di soluzioni rivolte all'hardening del sistema come SELinux e GRSecurity, ritieni che ci sia ancora "terreno di battaglia" per progetti come "rkhunter"?

M. Boelen: Il futuro di Rootkit Hunter non risentirà direttamente di queste soluzioni perché ognuna di essa ha i propri propositi. Una grande differenza, ad esempio, è quella che si ha effettuando l'analisi di un sistema compromesso quando, sia SELinux che GRSecurity, cercano, in primo luogo, di evitare di eseguire istruzioni non autorizzate (NDA: offrendo di fatto un modo preventivo per rendere sicuro un sistema). Questo offre ad ogni applicativo l'opportunità di sperimentare scenari differenti. Il punto forte di Rootkit Hunter è la ricerca di malware estremamente specifico, che può tradursi in vulnerabilità per il sistema. Vi sono determinati software dannosi nati con l'unico intento di evitare di essere rilevati (spesso fino alla release successiva) che, ad esempio, dimostrano ancora che questo tipo di situazioni è come il gioco del gatto e del topo. Personalmente ho notato un cambiamento nella tipologia di attacchi informatici condotti. Le vulnerabilità di tipo SQL Injection o relative ad errori di programmazioni presenti nei software sembrano essere incrementate molto nel corso di questi 7/8 anni mentre il numero di rootkit decresce. Quale autore originario di Rootkit Hunter penso sia difficile predire quale sia il futuro di questo progetto. Questo perché lo sviluppo dello stesso è condotto da un team e la mia attenzione è passata prevalentemente a Lynis. Il secondo motivo è quello che non sapremo mai quando nuove e più intelligenti forme di malware improvvisamente vedranno luce. Per ora Rootkit Hunter riempie un gap e continuerà a farlo per almeno qualche anno.

Giovanni Federico

FILO DIRETTO

Diversamente da molti altri "guru" dell'IT con cui gli utenti hanno a che fare, Michael è tutto fuorché irraggiungibile. Come traspare da questa intervista, mister Boelen è, invece, molto felice di lasciarsi intervistare e chiacchierare di quelli che, in fondo, sono interessi comuni. Lui, certo, ha un punto di vista privilegiato, da addetto del settore ai massimi livelli. Non per questo sembra tirarsi indietro quando si tratta di informare gli altri di problemi seri e coinvolgenti. Una sua risposta, quindi, non può essere garantita ma non si ritiene parte di un olimpo irraggiungibile come fanno altri. Per contattarlo, ovviamente, basta visitare il sito www.rootkit.nl e usare il modulo. Se il suo lavoro ci piace, diamo un'occhiata alla sua wishlist su Amazon: adora leggere.

SLIC Table

Windows 7 usa gli stessi meccanismi di attivazione di Vista...

Appena iniziate le vendite ufficiali di Windows7 già si sono trovati in giro i primi crack. Il nodo sono le SLIC Table, la difesa che scelta da Microsoft per proteggere i suoi prodotti fin da Windows Vista che era stato già rapidamente aggirato. Certamente noi non siamo interessati a capire come evitare di pagare una regolare licenza, ma vediamo come è stato possibile aggirare le nuove protezioni.

:: La SLIC Table

Già ad agosto, dei pirati cinesi sono entrati in possesso di una versione OEM del dvd di Windows7 RTM per pc Lenovo. Queste versioni sono realizzate appositamente per pc che sono venduti direttamente con il sistema operativo a bordo, pre-attivato o quasi. Il caso ha voluto che tale versione includesse le nuove protezioni (non incluse nelle beta precedenti), il che ha dato un indubbio vantaggio ai cracker per rendersi conto di quali misure erano state adottate ed essere pronti per il rilascio della versione ufficiale. Rispetto a Vista, Microsoft ha infatti aggiornato il sistema di blocco SLP (System-Locked Preinstallation) alla versione 2.1 per supportare oltre Windows7 anche Windows Server 2008 ed è richiesto che una porzione di BIOS, chiamata SLIC Table e inserita all'interno del modulo ACPI (Advanced Configuration and Power Interface) contenga una firma digitale che corrisponda tramite un algoritmo alla chiave inserita dall'utente alla prima attivazione del sistema operativo. Tale protezione è studiata soprattutto per i BIOS dei notebook venduti con Windows7 e il dvd per Lenovo supportava esattamente questo schema di protezione. Apparentemente efficace, si è invece rivelata una protezione abbastanza debole dato che gli aggiornamenti di bios sono alla portata di molte persone e anche il relativo crack è simile a quan-

X-Ways, www.x-ways.net, offre software forense molto interessante...

Le specifiche di ogni produttore di computer sono facilmente recuperabili...

to già utilizzato per Vista e talmente efficace da ingannare il Genuine Advantage. Ad esempio, per aggirare la protezione nel caso il bios non fosse così recente, si potrà modificarlo per inserire la SLIC table e successivamente andranno modificati OEM ID e OEM TABLE ID per rispecchiare il certificato digitale corrispondente. Una volta estratto il certificato OEM e la chiave OEM di prodotto, è stato possibile confermare che Windows7 utilizza la stessa firma digitale del certificato OEM che era già usata in Windows Vista, il che ha permesso ai cracker di procedere su una strada già battuta e andare oltre: le chiavi estratte dai recenti bios permettono virtualmente di attivare tutte le copie di Windows7 OEM, anche di produttori diversi da Lenovo, fintanto che l'OEMID resta lo stesso. La combinazione corretta di Chiave Privata, Chiave Pubblica con OEMID, passerà infatti la validazione della licenza Microsoft rendendo la copia autorizzata a connettersi a Windows Update e ingannare il Genuine Validation.

:: Come aggirare la protezione

Le strade sono diverse e si può agire in hardware (hardmod) o in bios (biosmod), o addirittura emulare o simulare la SLIC Table durante il boot di windows (softmod). Nel caso del biosmod,va modificato il BIOS per includere le SLIC 2.1 ed è stata inizialmente la soluzione più adottata, con la raccolta in tutta la rete dei binari di migliaia di diversi bios recenti, con la speranza di rintracciare il nuovo codice e soprattutto le chiavi digitali. Sono stati così recuperati i binari delle SLIC table 2.1 da diversi nuovi notebook che supportano l'aggiornamento gratuito da Windows Vista a Windows 7 ed è addirittura possibile ricevere assistenza in forum su come realizzare un softmod. Certo, mettere mano al BIOS può invalidarne la garanzia e nei casi peggiori possiamo persino rischiare di rendere non funzionante la motherboard se qualcosa va storto durante il flashing. Il passo successivo a modificare direttamente il BIOS battuto dai pirati è stato quindi quello di emularlo nel momento in cui Windows7 controlla che rispetti lo standard SLP 2, ossia al suo avvio. Sono nati così dei "loader" di Windows7 che intervengono in questa fase; forse il più famoso si chiama proprio "Windows 7 Loader" e gestisce anche un elenco di seriali continuamente aggiornato per superare anche il problema della black-list di Microsoft.

:: Come recuperano le SLIC Table dal BIOS?

Se si possiede un BIOS che contiene un'autentica SLIC table (normalmente vero se abbiamo Windows Vista preinstallato), si può procedere manualmente ad estrarre e salvare le SLIC table in un file per studiarle o per tenercelo da parte come backup, nel caso un malaugurato giorno dovessimo averne bisogno. Dobbiamo tenere presente che , senza essere maliziosi,la nostra regolare licenza dipende da queste chiavi. Quindi è meglio premunirsi, no?

ePro Tek produce HWDirect, per l'accesso a basso livello ai registri hardware.

Gli accordi con alcuni produttori costano a Microsoft un crack di classe.

I passi da seguire sono i seguenti:

1. scaricare un tool per fare il dump macroscopico del BIOS come Everest Ultimate Edition (UE, www.lavalys.com/products/overview.php?pid=3&ps=UE&lang=en) e un tool che permette di accedere a basso livello come HWDirect (www.eprotek.com/download.html)
2. lanciare Everest, selezionare "Motherboard" poi "ACPI" e vedremo visualizzate tutte le tabelle presenti nel modulo ACPI
3. cliccare sulla SLIC table e nel pannello inferiore verrano visualizzate tutte le informazioni relative; annota l'indirizzo di memoria (es. "3F7D1F90") e la lunghezza o dimensione della tabella; la dimensione che soddisfa i requisiti di SLP 2.x è 374 bytes (176h)
4. lanciare ora HWDirect e selezionare "Memory Dump"; si aprirà un pop-up e sotto "Physical Address" inserire l'indirizzo precedentemente annotato (es. "3F7D1F90"); nel campo "Size" inserire 176 come lunghezza e premere Dump; la memoria verrà letta e visualizzata nel pannello "Memory Dump" e per verificarne la correttezza basta osservare che i primi quattro byte corrispondano alle lettere "SLIC"; cliccare quindi su "Save" per salvarlo in un file (es. ACPISLIC.BIN).

Con lo stesso metodo può essere salvata anche la tabella RSDT.

NoeXKuzE